Semester II Examinations 2009/2010

Exam Codes	3BA1, 4BA4, 4BS3, 4CS2
Exams	Bachelor of Arts Degree Bachelor of Science Degree
Module	Ring Theory and Field Theory
Module Code	MA416 and MA491
External Examiner	Professor D. Armitage
Internal Examiner(s)	Professor T. Hurley Dr R. Quinlan Dr J. Ward
Instructions:	In Section A, answer *seven* of the ten parts of Question A1 and *one* of Questions A2 and A3. In Section B, answer *seven* of the eleven parts of Question B1 and *one* of Questions B2 and B3.
Duration	Three Hours
No. of Pages	Four pages, including this one.
Department(s)	Mathematics
Requirements:	No special requirements
Release to Library:	Yes

Section A – Ring Theory (MA416)

A1. Answer *seven* of the following ten questions.

(a) Determine whether each of the following is a ring. If you believe that the object *is* a ring, it is enough to just say so. If not, you should give a reason why not.

i. The set of *upper triangular* 3×3 matrices with entries in the field $\mathbb{R}$ of real numbers, with the usual addition and multiplication of matrices. (Recall that a square matrix A is *upper triangular* if $A_{ij} = 0$ whenever $i > j$.)

ii. The set of *symmetric* 2×2 matrices with entries in the field $\mathbb{Q}$ of rational numbers, under the usual addition and multiplication of matrices. (Recall that a square matrix is *symmetric* if it is equal to its transpose).

iii. The set of polynomials in $\mathbb{Q}[x]$ with non–negative constant term, under the usual addition and multiplication of polynomials.

(b) Let R be the ring of functions from $\mathbb{R}$ to $\mathbb{R}$, with addition $(+)$ and multiplication $(\times)$ defined as follows, for $f, g \in R$.

$$(f+g)(x) = f(x) + g(x), \text{ for } x \in \mathbb{R}, \qquad (f \times g)(x) = f(x) \times g(x), \text{ for } x \in \mathbb{R}.$$

i. Is the multiplication in R commutative? Explain your answer.

ii. What is the identity element for multiplication in R?

iii. Give an example of a non–constant function that is a unit in R. Describe the inverse of this element for multiplication.

iv. Characterize those elements of R that are *not* units.

(c) Let R be a commutative ring with identity. What is meant by a *zero-divisor* in R? Show that no unit in R can be a zero-divisor in R. Must every non-zero element of R be either a zero-divisor or a unit? Explain your answer.

(d) What is meant by a *field*? Write down three different examples of fields.
Let F be a field. State the division algorithm for the polynomial ring $F[x]$.
Suppose that $f(x) \in F[x]$ has degree at least 1, and that $x - \alpha$ is a factor of $f(x)$ in $F[x]$, for some $\alpha \in F$. Show that α is a *root* of $f(x)$.

(e) What is meant by a *primitive* polynomial in $\mathbb{Z}[x]$? Prove that the product of two primitive polynomials in $\mathbb{Z}[x]$ is again primitive.

(f) Let F be a field. What is meant by an *irreducible* polynomial in $F[x]$?
Show that it is possible for an irreducible polynomial in $F[x]$ to be reducible over a field E that contains F as a subfield.
Give an example of an irreducible quadratic polynomial in $\mathbb{R}[x]$.
Give an example of a field F and a polynomial in $F[x]$ that has no root in F but is reducible in $F[x]$.

(g) Determine, with explanation, whether each of the following polynomials is irreducible in the indicated ring.

i. $-2x^4 - 3x^3 + 5x^2 + 4x - 4$, in $\mathbb{Z}[x]$

ii. $x^5 - \frac{5}{3}x^3 + \frac{17}{50}x^2 - \frac{5}{7}x + \frac{1}{3}$, in $\mathbb{R}[x]$

iii. $4x^6 - 15x^4 + 9x^3 - 18x^2 - 12x + 30$, in $\mathbb{Q}[x]$

iv. $2x^3 + 3x + 1$, in $\mathbb{Q}[x]$

v. $x^2 + 1$, in $\mathbb{F}_3[x]$, where $\mathbb{F}_3$ denotes the field $\mathbb{Z}/3\mathbb{Z}$ of integers modulo 3.

(h) Let R and S be commutative rings. What does it mean to say that a function $\phi : R \longrightarrow S$ is a *ring homomorphism?*
If $\phi : R \longrightarrow S$ is a ring homomorphism, define the *image* of ϕ and prove that it is a subring of S.
If x is a zero-divisor in R, must $\phi(x)$ be a zero-divisor in S?

(i) Let R be a commutative ring. What is meant by an *ideal* of R?
What is meant by a *principal ideal* of R? Prove that every ideal of the ring $\mathbb{Z}$ of integers is principal.
Give an example, with explanation, of a commutative ring with identity R and an ideal of R that is not principal.

(j) Let R be a commutative ring with identity.
What is meant by a *maximal* ideal in R?
Prove that an ideal I of R is maximal if and only if the factor ring R/I is a field.

A2. Write a note of two to three pages in length on the subject of multiplication in the rings $\mathbb{Z}/n\mathbb{Z}$ of integers modulo n. Your note should contain the following :

- A description of the elements of $\mathbb{Z}/n\mathbb{Z}$ for a natural number n.
- An explanation of how multiplication in $\mathbb{Z}/n\mathbb{Z}$ is defined.
- Descriptions, with proof, of which elements of $\mathbb{Z}/n\mathbb{Z}$ are units and which are zero-divisors.

A3. Write a two to three page note on *Eisenstein's Irreducibility Criterion*. Your account should include a statement of Eistenstein's Irreducibility Criterion and at least two of the following :

- A proof of Eistenstein's Irreducibility Criterion
- A proof of a variant of Eisenstein's Irreducibility Criterion, in which the prime p divides all the coefficients except the constant coefficient, and p^2 does not divide the leading coefficient.
- A proof that the polynomial $x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible in $\mathbb{Q}[x]$ if p is prime.
- A biographical note about Gotthold Eisenstein.

Section B – Field Theory (MA 491)

B1. Answer **seven** of the following eleven parts.

(a) Explain how a field $\mathbb{K}$ may be viewed as a vector space over a sub–field $\mathbb{F}$ and hence define the **degree** $[\mathbb{K} : \mathbb{F}]$.

(b) Determine the degree of the extension $\left[\mathbb{Q}\left(\sqrt{11+6\sqrt{2}}\right) : \mathbb{Q}\right]$.

(c) If the degree of u over the field $\mathbb{K}$ is odd, prove that $\mathbb{K}(u) = \mathbb{K}(u^2)$.

(d) Show that $\mathbb{Q}(i, \sqrt{2})$ is the splitting field of the polynomial $f(x) = x^4 - x^2 - 2$ over $\mathbb{Q}$.

(e) Verify that $\Phi_8(x)\,(= x^4 + 1)$ factorises (reduces) in $\mathbb{Q}(\sqrt{2}i)$, where $i = \sqrt{-1}$.

(f) Let p be an **odd** prime. Show that $\Phi_{2p}(x) = \Phi_p(-x)$.

(g) Prove that for $n \geq 2$, $\Phi_n(x)$ is a **reciprocal** polynomial, in that $\Phi_n(x) = x^k \Phi_n\left(\frac{1}{x}\right)$ where $k = \phi(n)$ is the degree of $\Phi_n(x)$.

(h) Show that $x^4 - 10x^2 + 1$ is **reducible**, (i.e. it can be factored) over $\mathbb{Q}(\sqrt{6})$. Show also that $x^4 - 10x^2 + 1$ is **reducible** over $\mathbb{Q}(\sqrt{3})$.

(i) State Gauss's Theorem concerning the values of n for which the regular n–gon can be constructed by straight edge and compass.

(j) **Prove** that the angle n° is constructible $\Leftrightarrow 3|n$.

(k) Show that $\cos^{-1}\left(\frac{118}{125}\right)$ can be trisected using straight–edge and compass.

B2. (i) Verify that $\Phi_8(x)\,(= x^4 + 1)$ factorises (reduces) in $\mathbb{Q}(\sqrt{2})$, and hence construct a splitting field for $x^4 + 1$ over $\mathbb{Q}$. If θ denotes a root of $\Phi_8(x)$, show that the other three roots are $\theta^{-1}, -\theta, -\theta^{-1}$.

(ii) Consider an automorphism of $\mathbb{Q}(\theta)$, α say, such that

$$\alpha : \theta \mapsto \theta^{-1}\,.$$

How does α act on the other three roots of $\Phi_8(x)$? If β is the automorphism defined by

$$\beta : \theta \mapsto -\theta$$

find the images under β of the other three roots. Show that $\alpha\beta = \beta\alpha$ and that the group of automorphisms $\langle \alpha, \beta \rangle$ is isomorphic with the Klein 4-group.

(iii) Check that $\mathbb{Q}(\sqrt{2})$ is the fixed field of α. Find the fixed fields of the automorphisms β and $\alpha\beta$ respectively, and show that $x^4 + 1$ is reducible over each of these intermediate fields.

B3. (i) Let $\mathbb{F}_q$ be a finite field of order q $(= p^n,\ p$ a prime $n \geq 1)$. State the main properties of $\mathbb{F}_q$.

(ii) Prove Gauss' formula

$$N_q(d) = \frac{1}{d} \sum_{k|d} \mu\left(\frac{d}{k}\right) q^k$$

where $N_q(d)$ is the number of monic irreducible polynomials of degree d over the finite field of order q.

(iii) By factorising $x^{16} - x$ over the field of two elements $\mathbb{F}_2$, or otherwise, determine the irreducible polynomials of degree 4 over the field of two elements $\mathbb{F}_2$.

(iv) Choosing any of the irreducible quartics in part (iii), show that it can be factored into a product of two irreducible quadratics over $\mathbb{F}_4$, the finite field of order 4.